UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/068,280	02/04/2002	Mark J. McArdle	01.239.01	9739

7590 09/11/2006

ZILKA-KOTAB PC
PO Box 721120
San Jose, CA 95172-1120

EXAMINER	
HA, LEYNNA A	

ART UNIT	PAPER NUMBER
2135	

DATE MAILED: 09/11/2006

Please find below and/or attached an Office communication concerning this application or proceeding.

UNITED STATES PATENT AND TRADEMARK OFFICE

Commissioner for Patents
United States Patent and Trademark Office
P.O. Box 1450
Alexandria, VA 22313-1450
www.uspto.gov

BEFORE THE BOARD OF PATENT APPEALS AND INTERFERENCES

Application Number: 10/068,280
Filing Date: February 04, 2002
Appellant(s): MCARDLE ET AL.

Kevin J. Zilka - Reg. No. 41,429
Of Zilka-Kotab, P.C.

For Appellant

EXAMINER'S ANSWER

This is in response to the appeal brief filed June 12, 2006 appealing from the Office action mailed November 15, 2005.

(1) Real Party in Interest

A statement identifying by name the real party in interest is contained in the brief.

(2) Related Appeals and Interferences

The examiner is not aware of any related appeals, interferences, or judicial proceedings which will directly affect or be directly affected by or have a bearing on the Board's decision in the pending appeal.

(3) Status of Claims

The statement of the status of claims contained in the brief is correct.

(4) Status of Amendments After Final

The appellant's statement of the status of amendments after final rejection contained in the brief is correct.

(5) Summary of Claimed Subject Matter

The summary of claimed subject matter contained in the brief is correct.

(6) Grounds of Rejection to be Reviewed on Appeal

The appellant's statement of the grounds of rejection to be reviewed on appeal is substantially correct. The changes are as follows:

a.) Claims 1-4, 7-12, 14-18, 21-26, 28-32, 34-40, 42-44, 47-48, and 50-51 are rejected under 35 U.S.C. 103(a) as being unpatentable over Freund (5,987,611) and in further view of Kaler, et al. (US 6,671,829).

b.) Claims 13, 27, 41, and 49 are rejected under 35 U.S.C. 103(a) as being unpatentable over Freund and Kaler, et al, and further in view of Official Notice.

NEW GROUND(S) OF REJECTION

c.) Claims 5-6, 19-20, 33-34, and 45-46 receive a new ground of rejection as being unpatentable over Freund and Kaler, and further in view Hanko, et al. (US 6,912,578).

(7) Claims Appendix

The copy of the appealed claims contained in the Appendix to the brief is correct.

(8) Evidence Relied Upon

5,987,611	Freund	11-1999
6,671,829	Kaler, et al.	12-2003
6,912,578	Hanko, et al.	6-2005

(9) Grounds of Rejection

The following ground(s) of rejection are applicable to the appealed claims:

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

1. **Claims 1-4, 7-12, 14-18, 21-26, 28-32, 34-40, 42-44, 47-48, and 50-51 are rejected under 35 U.S.C. 103(a) as being unpatentable over Freund (5,987,611) and in further view of Kaler, et al. (US 6,671,829).**

As per claim 1:

Freund teaches a computerized method comprising:

determining an active networked application; **[col.4, lines 34-37 and col.10, lines 31-44 and col.30, lines 13-15]**

filtering a set of intrusion rules to create a subset of intrusion rules **[col.5, lines 41-43 and 53-59]** corresponding to the active networked application **[col.4,**

lines 7-18 and 41-57], where the subset of the intrusion rules corresponding to the active networked application are capable of being used for evaluating intrusions that target the corresponding active networked application; and **[col.8, lines 45-52 and col.11, lines 5-18]**

evaluating network traffic using the subset of intrusion rules **[col.10, lines 55-65 and col.12, lines 55-65];**

wherein the subset of the intrusion rules corresponding to the active networked application are used for evaluation for reducing a required amount of processing resources. **[col.13, lines 59-65]**

Although, the subset of intrusion rules was disclosed, Freund did not fully explain the details of the subset of intrusion rules such that they reduce the required amount of processing the resources.

Kaler, et al. teaches the an invention that includes a number of different aspects for analyzing the performance of a data processing system wherein provides the filtering process and filter reduction feature. Kaler disclose the filter defines what information it (VSA) will collect and analyze (col.23, lines 14-15) and the filter reduction is the process of modifying or creating a new version of a Boolean expression (col.23, lines 45-65) whereby extracts only the information of interest so that it reduces the performance impact of monitoring or processing resources (col.4, lines 57-61).

Therefore, it would have been obvious for a person of ordinary skills in the art to combine the teaching the subset of intrusion rules of Freund with the teaching of filter reduction to extract only the information of interest as taught by Kaler because this reduces the performance impact of monitoring.

As per claim 2: See Freund on col.4, lines 51-62; discusses detecting when the active networked application becomes inactive and re-filtering the set of intrusion rules.

As per claim 3: See Freund on col.13, lines 52-55; discusses monitoring network connection terminations.

As per claim 4: See Freund on col.13, lines 20-22; discusses monitoring application terminations.

As per claim 7: See Freund on col.10, lines 31-44 and col.30, lines 13-15; discusses detecting when a network connection for an active application is initiated.

As per claim 8: See Freund on col.5, lines 46-59 and col.13, lines 50-56; discusses marking an intrusion rule corresponding to the active networked application.

As per claim 9: See Freund on col.4, lines 65-67 and col.5, lines 39-43; discusses extracting the subset of rules into an optimized set of rules.

As per claim 10: See Freund on col.12, lines 3-5; discusses analyzing network traffic on a port specified in the subset of rules.

As per claim 11: See Freund on col.4, lines 65-67 and col.5, lines 39-43; discusses analyzing network traffic for a protocol specified in the subset of rules.

As per claim 12: See Freund on col.13, lines 15-22; discusses discarding network traffic that satisfies at least one of the subset of rules and reporting an intrusion attempt.

As per claim 14: See Freund on col.4, lines 65-67 and col.5, lines 39-43; discusses the set of intrusion rules comprises heuristic rules.

As per claim 15:

discusses a computer-readable medium having executable instructions to cause a computer to perform a method comprising:

determining an active networked application; **[col.4, lines 34-37 and col.10, lines 31-44 and col.30, lines 13-15]**

filtering a set of intrusion rules to create a subset of intrusion rules **[col.5, lines 41-43 and 53-59]** corresponding to the active networked application **[col.4, lines 7-18 and 41-57]**, where the subset of the intrusion rules corresponding to the active networked application are capable of being used for evaluating intrusions that target the corresponding active networked application; and **[col.8, lines 45-52 and col.11, lines 5-18]**

evaluating network traffic using the subset of intrusion rules **[col.10, lines 55-65 and col.12, lines 55-65]**;

wherein the subset of the intrusion rules corresponding to the active networked application are used for evaluation for reducing a required amount of processing resources. **[col.13, lines 59-65]**

Although, the subset of intrusion rules was disclosed, Freund did not fully explain the details of the subset of intrusion rules such that they reduce the required amount of processing the resources.

Kaler, et al. teaches the an invention that includes a number of different aspects for analyzing the performance of a data processing system wherein provides the filtering process and filter reduction feature. Kaler disclose the filter defines what information it (VSA) will collect and analyze (col.23, lines 14-15) and the filter reduction is the process of modifying or creating a new version of a Boolean expression (col.23, lines 45-65) whereby extracts only the

information of interest so that it reduces the performance impact of monitoring or processing resources (col.4, lines 57-61).

Therefore, it would have been obvious for a person of ordinary skills in the art to combine the teaching the subset of intrusion rules of Freund with the teaching of filter reduction to extract only the information of interest as taught by Kaler because this reduces the performance impact of monitoring.

As per claim 16: See Freund on col.4, lines 51-62; discusses detecting when the active networked application becomes inactive, and re-filtering the set of intrusion rules.

As per claim 17: See Freund on col.13, lines 20-22; discusses monitoring network connection terminations.

As per claim 18: See Freund on col.13, lines 20-22; discusses the detecting comprises monitoring application terminations.

As per claim 21: See Freund on col.10, lines 31-44 and col.30, lines 13-15; discusses detecting when an active application initiates a network connection.

As per claim 22: See Freund on col.5, lines 46-59 and col.13, lines 50-56; discusses marking an intrusion rule corresponding to the active networked application.

As per claim 23: See Freund on col.4, lines 65-67 and col.5, lines 39-43; discusses extracting the subset of rules into an optimized set of rules.

As per claim 24: See Freund on col.12, lines 3-5; discusses analyzing network traffic on a port specified in the subset of rules.

As per claim 25: See Freund on col.4, lines 65-67 and col.5, lines 39-43; discusses analyzing network traffic for a protocol specified in the subset of rules.

As per claim 26: See Freund on col.13, lines 15-22; discusses discarding network traffic that satisfies at least one of the subset of rules; and reporting an intrusion attempt.

As per claim 28: See Freund on col.4, lines 65-67 and col.5, lines 39-43; discusses the set of intrusion rules comprises heuristic rules.

As per claim 29:

discusses a system comprising:

a processor coupled to a memory through a bus; and **[col.7, lines 40-51]**

an intrusion prevention process executed from the memory by the processor to cause the processor to determine an active networked application **[col.4, lines 34-37 and col.10, lines 31-44 and col.30, lines 13-15]**, to filter a set of intrusion rules to create a subset of rules corresponding to the active networked application **[col.4, lines 7-18 and 41-57]**, where the subset of the intrusion rules **[col.5, lines 41-43 and 53-59]** corresponding to the active networked application are capable of being used for evaluating intrusions that target the corresponding active networked application **[col.8, lines 45-52 and col.11, lines 5-18]** and to evaluate network traffic using the subset of intrusion rules **[col.10, lines 55-65 and col.12, lines 55-65]**;

wherein the subset of the intrusion rules corresponding to the active networked application are used for evaluation for reducing a required amount of processing resources. **[col.13, lines 59-65]**

Although, the subset of intrusion rules was disclosed, Freund did not fully explain the details of the subset of intrusion rules such that they reduce the required amount of processing the resources.

Kaler, et al. teaches the an invention that includes a number of different aspects for analyzing the performance of a data processing system wherein provides the filtering process and filter reduction feature. Kaler disclose the filter defines what information it (VSA) will collect and analyze (col.23, lines 14-15) and the filter reduction is the process of modifying or creating

a new version of a Boolean expression (col.23, lines 45-65) whereby extracts only the information of interest so that it reduces the performance impact of monitoring or processing resources (col.4, lines 57-61).

Therefore, it would have been obvious for a person of ordinary skills in the art to combine the teaching the subset of intrusion rules of Freund with the teaching of filter reduction to extract only the information of interest as taught by Kaler because this reduces the performance impact of monitoring.

As per claim 30: See Freund on col.4, lines 51-62; discusses the intrusion prevention process further causes the processor to detect when the active networked application becomes inactive, and to re-filter the set of intrusion rules.

As per claim 31: See col., lines ; discusses the intrusion prevention process further causes the processor to monitor network connection terminations in detecting when the active networked application becomes inactive.

As per claim 32: See col., lines ; discusses the intrusion prevention process further causes the processor to monitor application terminations in detecting when the active networked application becomes inactive.

As per claim 35: See Freund on col.10, lines 31-44 and col.30, lines 13-15; discusses the intrusion prevention process further causes the processor to detect when an active application initiates a network connection in determining an active networked application.

As per claim 36: See Freund on col.5, lines 46-59 and col.13, lines 50-56; discusses the intrusion prevention process further causes the processor to mark an intrusion rule corresponding to the active networked application in filtering the set of intrusion rules.

As per claim 37: See Freund on col.4, lines 65-67 and col.5, lines 39-43; discusses the intrusion prevention process further causes the processor to extract the subset of rules into an optimized set of rules in filtering the set of intrusion rules.

As per claim 38: See Freund on col.12, lines 3-5; discusses the intrusion prevention process further causes the processor to analyze network traffic on a port specified in the subset of rules in evaluating the network traffic.

As per claim 39: See Freund on col.4, lines 65-67 and col.5, lines 39-43; discusses the intrusion prevention process further causes the processor to analyze network traffic for a protocol specified in the subset of rules in evaluating the network traffic.

As per claim 40: See Freund on col.13, lines 15-22; discusses the intrusion prevention process further causes the processor to discard network traffic that satisfies at least one of the subset of rules, and to report an intrusion attempt in evaluating the network traffic.

As per claim 42: See Freund on col.4, lines 65-67 and col.5, lines 39-43; discusses the set of intrusion rules comprises heuristic rules.

As per claim 43:

discusses an apparatus comprising:

means for determining when an active application becomes an active networked application; **[col.4, lines 34-37 and col.10, lines 31-44 and col.30, lines 13-15]**

means for filtering a set of intrusion rules to create a subset of intrusion rules corresponding to the active networked application **[col.4, lines 7-18 and 41-57]**, where the subset of the intrusion rules **[col.5, lines 41-43 and 53-59]** corresponding to the active networked application are capable of being used for evaluating intrusions that target the corresponding active networked application; and **[col.8, lines 45-52 and col.11, lines 5-18]**

means for evaluating coupled to the means for filtering to evaluate network traffic using the subset of intrusion rules **[col.10, lines 55-65 and col.12, lines 55-65]**;

wherein the subset of the intrusion rules corresponding to the active networked application are used for evaluation for reducing a required amount of processing resources. **[col.13, lines 59-65]**

Although, the subset of intrusion rules was disclosed, Freund did not fully explain the details of the subset of intrusion rules such that they reduce the required amount of processing the resources.

Kaler, et al. teaches the an invention that includes a number of different aspects for analyzing the performance of a data processing system wherein provides the filtering process and filter reduction feature. Kaler disclose the filter defines what information it (VSA) will collect and analyze (col.23, lines 14-15) and the filter reduction is the process of modifying or creating a new version of a Boolean expression (col.23, lines 45-65) whereby extracts only the information of interest so that it reduces the performance impact of monitoring or processing resources (col.4, lines 57-61).

Therefore, it would have been obvious for a person of ordinary skills in the art to combine the teaching the subset of intrusion rules of Freund with the teaching of filter reduction to extract only the information of interest as taught by Kaler because this reduces the performance impact of monitoring.

As per claim 44: See Freund on col.4, lines 51-62; discusses the means for determining further detects when the active networked application becomes inactive and the means for filtering further re-filters the set of intrusion rules when the active networked application becomes inactive.

As per claim 47: See Freund on col.13, lines 15-22; discusses means for discarding network traffic that satisfies at least one of the subset of rules; and means for reporting an intrusion attempt.

As per claim 48: See Freund on col.11, line 56 – col.12, line 17 and col.13, lines 13-22; discusses intrusion rules include information selected from the group consisting of a targeted active networked application, a specific hostile payload, a network port, and a protocol.

As per claim 50: See Freund on col.4, lines 65-67 and col.5, lines 39-43; discusses the set of intrusion rules comprises heuristic rules.

As per claim 51: See Freund on col.13, lines 34-42 and col.23, lines 20-22 and 52-55; discusses the heuristic rule includes information associated with an active networked application making a new connection never previously made.

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

2. Claims 5, 6, 19, 20, 33, 34, 45, and 46 are rejected under 35 U.S.C. 103(a) as being unpatentable over Freund and Kaler and further in view of Hanko, et al. (US 6,912,578).

As per claim 5:

Freund teaches a system and method for client based monitoring and filtering (col.3, lines 50-67). Freund discloses that applications (software) can be a Web browser (i.e.

Netscape Navigator or Microsoft Internet Explorer) which communicates with the Internet (col.8, lines 2-10 and col.15, lines 14-21). An active application is where active use occurs when a user directly interacts with an Internet application while that application accesses the Internet (col.10, lines 17-43). Freund discloses client-based filter application performs all of the monitoring, logging, filter work, and also keeps a list of currently active processes and determines which process is actively used (col.4, lines 31-37). Freund discloses the system can monitor TCP/IP activities on a per process or per application basis and it access rights (col.4, lines 52-55). Freund discloses the set of intrusion rules are access rules for the entire LAN for one or more workgroups, or the specific user (col.3, lines 61-63).

Kaler indicates there is a substantial need to provide automated tools for efficiently analyzing the performance, function and behavior of their applications without significantly affecting the performance or data security characteristics of the applications (col.3, lines 39-45). Kaler disclose the filter defines what information it (VSA) will collect and analyze (col.23, lines 14-15) and the filter reduction is the process of modifying or creating a new version of a Boolean expression (col.23, lines 45-65) whereby extracts only the information of interest so that it reduces the performance impact of monitoring or processing resources (col.4, lines 57-61).

The Freund and Kaler combination did not include detecting when no networked application is active, and suspending the evaluating of network traffic until a networked application is active.

Hanko, et al. teaches a method and apparatus for improving utilization of one or more resources in a share client computer environment (col.3, lines 30-32). Hanko points out that on a consolidated client system, a small load may be multiplied by tens, hundreds, or even millions of users of the shared system, can consume all of the resources of the shared system, even when no real work is being done (col.5, lines 1-8). Hanko discloses using traditional computer

programs on a shared client by monitoring the status of an application, determining when an application no longer needs resources and causing the application to stop consuming resources (col.3, lines 34-37). The invention has a mechanism to stop a program from consuming resources when it detects a user has stopped interaction with an application and to restart it when the user begins interaction with it (col.5, lines 21-28). When there is no interaction regarding the application obviously becomes an inactive application (col.5, lines 10-13). This inactive application no longer consumes resources obviously no longer is being evaluated or suspended for the time being until the application returns to its original (active) state again (col.12, lines 33-45 and 55-62).

Therefore, it would have been obvious for a person of ordinary skills in the art at the time of the invention was made to combine the teaching of monitoring and filtering with intrusion rules of the Freund and Kaler combination with the teaching of causing the application to stop consuming resources when detecting an application is inactive and to restart when the application active (col.3, lines 45-52) because this improves resource utilization (col.4, lines 16-17).

As per claim 6: See Hanko on col.12, lines 46-53; discusses continuing the evaluating of network traffic if no networked application is active.

As per claim 19:

Freund teaches a system and method for client based monitoring and filtering (col.3, lines 50-67). Freund discloses that applications (software) can be a Web browser (i.e. Netscape Navigator or Microsoft Internet Explorer) which communicates with the Internet (col.8, lines 2-10 and col.15, lines 14-21). An active application is where active use occurs when a user directly interacts with an Internet application while that application accesses the Internet (col.10, lines 17-43). Freund discloses client-based filter application performs all of the

monitoring, logging, filter work, and also keeps a list of currently active processes and determines which process is actively used (col.4, lines 31-37). Freund discloses the system can monitor TCP/IP activities on a per process or per application basis and it access rights (col.4, lines 52-55). Freund discloses the set of intrusion rules are access rules for the entire LAN for one or more workgroups, or the specific user (col.3, lines 61-63).

Kaler indicates there is a substantial need to provide automated tools for efficiently analyzing the performance, function and behavior of their applications without significantly affecting the performance or data security characteristics of the applications (col.3, lines 39-45). Kaler disclose the filter defines what information it (VSA) will collect and analyze (col.23, lines 14-15) and the filter reduction is the process of modifying or creating a new version of a Boolean expression (col.23, lines 45-65) whereby extracts only the information of interest so that it reduces the performance impact of monitoring or processing resources (col.4, lines 57-61).

The Freund and Kaler combination did not include detecting when no networked application is active, and suspending the evaluating of network traffic until a networked application is active.

Hanko, et al. teaches a method and apparatus for improving utilization of one or more resources in a share client computer environment (col.3, lines 30-32). Hanko points out that on a consolidated client system, a small load may be multiplied by tens, hundreds, or even millions of users of the shared system, can consume all of the resources of the shared system, even when no real work is being done (col.5, lines 1-8). Hanko discloses using traditional computer programs on a shared client by monitoring the status of an application, determining when an application no longer needs resources and causing the application to stop consuming resources (col.3, lines 34-37). The invention has a mechanism to stop a program from consuming resources when it detects a user has stopped interaction with an application and to restart it

when the user begins interaction with it (col.5, lines 21-28). When there is no interaction regarding the application obviously becomes an inactive application (col.5, lines 10-13). This inactive application no longer consumes resources obviously no longer is being evaluated or suspended for the time being until the application returns to its original (active) state again (col.12, lines 33-45 and 55-62).

Therefore, it would have been obvious for a person of ordinary skills in the art at the time of the invention was made to combine the teaching of monitoring and filtering with intrusion rules of the Freund and Kaler combination with the teaching of causing the application to stop consuming resources when detecting an application is inactive and to restart when the application active (col.3, lines 45-52) because this improves resource utilization (col.4, lines 16-17).

As per claim 20: See Hanko on col.12, lines 46-53; discusses continuing the evaluating of network traffic if no networked application is active.

As per claim 33:

Freund teaches a system and method for client based monitoring and filtering (col.3, lines 50-67). Freund discloses that applications (software) can be a Web browser (i.e. Netscape Navigator or Microsoft Internet Explorer) which communicates with the Internet (col.8, lines 2-10 and col.15, lines 14-21). An active application is where active use occurs when a user directly interacts with an Internet application while that application accesses the Internet (col.10, lines 17-43). Freund discloses client-based filter application performs all of the monitoring, logging, filter work, and also keeps a list of currently active processes and determines which process is actively used (col.4, lines 31-37). Freund discloses the system can monitor TCP/IP activities on a per process or per application basis and it access rights (col.4,

lines 52-55). Freund discloses the set of intrusion rules are access rules for the entire LAN for one or more workgroups, or the specific user (col.3, lines 61-63).

Kaler indicates there is a substantial need to provide automated tools for efficiently analyzing the performance, function and behavior of their applications without significantly affecting the performance or data security characteristics of the applications (col.3, lines 39-45). Kaler disclose the filter defines what information it (VSA) will collect and analyze (col.23, lines 14-15) and the filter reduction is the process of modifying or creating a new version of a Boolean expression (col.23, lines 45-65) whereby extracts only the information of interest so that it reduces the performance impact of monitoring or processing resources (col.4, lines 57-61).

The Freund and Kaler combination did not include detecting when no networked application is active, and suspending the evaluating of network traffic until a networked application is active.

Hanko, et al. teaches a method and apparatus for improving utilization of one or more resources in a share client computer environment (col.3, lines 30-32). Hanko points out that on a consolidated client system, a small load may be multiplied by tens, hundreds, or even millions of users of the shared system, can consume all of the resources of the shared system, even when no real work is being done (col.5, lines 1-8). Hanko discloses using traditional computer programs on a shared client by monitoring the status of an application, determining when an application no longer needs resources and causing the application to stop consuming resources (col.3, lines 34-37). The invention has a mechanism to stop a program from consuming resources when it detects a user has stopped interaction with an application and to restart it when the user begins interaction with it (col.5, lines 21-28). When there is no interaction regarding the application obviously becomes an inactive application (col.5, lines 10-13). This inactive application no longer consumes resources obviously no longer is being evaluated or

suspended for the time being until the application returns to its original (active) state again (col.12, lines 33-45 and 55-62).

Therefore, it would have been obvious for a person of ordinary skills in the art at the time of the invention was made to combine the teaching of monitoring and filtering with intrusion rules of the Freund and Kaler combination with the teaching of causing the application to stop consuming resources when detecting an application is inactive and to restart when the application active (col.3, lines 45-52) because this improves resource utilization (col.4, lines 16-17).

As per claim 34: See Hanko on col.12, lines 46-53; discusses the intrusion prevention process further causes the processor to further filter the intrusion rules based on an operating system and to continue evaluating network traffic if no networked application is active.

As per claim 45:

Freund teaches a system and method for client based monitoring and filtering (col.3, lines 50-67). Freund discloses that applications (software) can be a Web browser (i.e. Netscape Navigator or Microsoft Internet Explorer) which communicates with the Internet (col.8, lines 2-10 and col.15, lines 14-21). An active application is where active use occurs when a user directly interacts with an Internet application while that application accesses the Internet (col.10, lines 17-43). Freund discloses client-based filter application performs all of the monitoring, logging, filter work, and also keeps a list of currently active processes and determines which process is actively used (col.4, lines 31-37). Freund discloses the system can monitor TCP/IP activities on a per process or per application basis and it access rights (col.4, lines 52-55). Freund discloses the set of intrusion rules are access rules for the entire LAN for one or more workgroups, or the specific user (col.3, lines 61-63).

Kaler indicates there is a substantial need to provide automated tools for efficiently analyzing the performance, function and behavior of their applications without significantly affecting the performance or data security characteristics of the applications (col.3, lines 39-45). Kaler disclose the filter defines what information it (VSA) will collect and analyze (col.23, lines 14-15) and the filter reduction is the process of modifying or creating a new version of a Boolean expression (col.23, lines 45-65) whereby extracts only the information of interest so that it reduces the performance impact of monitoring or processing resources (col.4, lines 57-61).

The Freund and Kaler combination did not include detecting when no networked application is active, and suspending the evaluating of network traffic until a networked application is active.

Hanko, et al. teaches a method and apparatus for improving utilization of one or more resources in a share client computer environment (col.3, lines 30-32). Hanko points out that on a consolidated client system, a small load may be multiplied by tens, hundreds, or even millions of users of the shared system, can consume all of the resources of the shared system, even when no real work is being done (col.5, lines 1-8). Hanko discloses using traditional computer programs on a shared client by monitoring the status of an application, determining when an application no longer needs resources and causing the application to stop consuming resources (col.3, lines 34-37). The invention has a mechanism to stop a program from consuming resources when it detects a user has stopped interaction with an application and to restart it when the user begins interaction with it (col.5, lines 21-28). When there is no interaction regarding the application obviously becomes an inactive application (col.5, lines 10-13). This inactive application no longer consumes resources obviously no longer is being evaluated or suspended for the time being until the application returns to its original (active) state again (col.12, lines 33-45 and 55-62).

Therefore, it would have been obvious for a person of ordinary skills in the art at the time of the invention was made to combine the teaching of monitoring and filtering with intrusion rules of the Freund and Kaler combination with the teaching of causing the application to stop consuming resources when detecting an application is inactive and to restart when the application active (col.3, lines 45-52) because this improves resource utilization (col.4, lines 16-17).

As per claim 46: See Hanko on col.12, lines 46-53; discusses the means for filtering further filters the intrusion rules corresponding to an operating system and the means for evaluating continues the evaluation of network traffic when the means for determining determines no networked application is active.

3. Claims 13, 27, 41, and 49 are rejected under 35 U.S.C. 103(a) as being unpatentable over Freund and Kaler, et al, and further in view of Official Notice.

As per claim 13:

Freund teaches a computerized method comprising determining an active networked application [col.10, lines 31-44 and col.30, lines 13-15] and filtering a set of intrusion rules to create a subset of intrusion rules corresponding to the active networked application [col.4, lines 65-67 and col.5, lines 39-43], where the subset of the intrusion rules corresponding to the active networked application are capable of being used for evaluating intrusions that target the corresponding active networked application [col.5, lines 46-59 and col.8, lines 45-52].

Kaler, et al. teaches the an invention that includes a number of different aspects for analyzing the performance of a data processing system wherein provides the filtering process and filter reduction feature. Kaler disclose the filter defines what information it (VSA) will collect and analyze (col.23, lines 14-15) and the filter reduction is the process of modifying or creating

a new version of a Boolean expression (col.23, lines 45-65) whereby extracts only the information of interest so that it reduces the performance impact of monitoring or processing resources (col.4, lines 57-61).

Freund and Kaler combinations did not include signature of known attacks in the set of intrusion rules. However, it is known in the art that signature of known attacks are also known as virus signatures. A signature is known as a unique computer code contained in a virus and that the signature for a known attacks or viruses is to identify infected programs or files and by knowing the signature of the attack will help find the antivirus program.

Therefore it would have been obvious for a person of ordinary skills in the art to combine the teachings of Freund and Kaler with Official Notice that signature of known viruses because the signature is for identifying infected programs from another signature in order to provide a solution or antivirus program.

As per claim 27:

Freund teaches a computerized method comprising determining an active networked application [col.10, lines 31-44 and col.30, lines 13-15] and filtering a set of intrusion rules to create a subset of intrusion rules corresponding to the active networked application [col.4, lines 65-67 and col.5, lines 39-43], where the subset of the intrusion rules corresponding to the active networked application are capable of being used for evaluating intrusions that target the corresponding active networked application [col.5, lines 46-59 and col.8, lines 45-52].

Kaler, et al. teaches the an invention that includes a number of different aspects for analyzing the performance of a data processing system wherein provides the filtering process and filter reduction feature. Kaler disclose the filter defines what information it (VSA) will collect and analyze (col.23, lines 14-15) and the filter reduction is the process of modifying or creating a new version of a Boolean expression (col.23, lines 45-65) whereby extracts only the

information of interest so that it reduces the performance impact of monitoring or processing resources (col.4, lines 57-61).

Freund and Kaler combinations did not include signature of known attacks in the set of intrusion rules. However, it is known in the art that signature of known attacks are also known as virus signatures. A signature is known as a unique computer code contained in a virus and that the signature for a known attacks or viruses is to identify infected programs or files and by knowing the signature of the attack will help find the antivirus program.

Therefore it would have been obvious for a person of ordinary skills in the art to combine the teachings of Freund and Kaler with Official Notice that signature of known viruses because the signature is for identifying infected programs from another signature in order to provide a solution or antivirus program.

As per claim 41:

Freund teaches a computerized method comprising determining an active networked application [col.10, lines 31-44 and col.30, lines 13-15] and filtering a set of intrusion rules to create a subset of intrusion rules corresponding to the active networked application [col.4, lines 65-67 and col.5, lines 39-43], where the subset of the intrusion rules corresponding to the active networked application are capable of being used for evaluating intrusions that target the corresponding active networked application [col.5, lines 46-59 and col.8, lines 45-52].

Kaler, et al. teaches the an invention that includes a number of different aspects for analyzing the performance of a data processing system wherein provides the filtering process and filter reduction feature. Kaler disclose the filter defines what information it (VSA) will collect and analyze (col.23, lines 14-15) and the filter reduction is the process of modifying or creating a new version of a Boolean expression (col.23, lines 45-65) whereby extracts only the

information of interest so that it reduces the performance impact of monitoring or processing resources (col.4, lines 57-61).

Freund and Kaler combinations did not include signature of known attacks in the set of intrusion rules. However, it is known in the art that signature of known attacks are also known as virus signatures. A signature is known as a unique computer code contained in a virus and that the signature for a known attacks or viruses is to identify infected programs or files and by knowing the signature of the attack will help find the antivirus program.

Therefore it would have been obvious for a person of ordinary skills in the art to combine the teachings of Freund and Kaler with Official Notice that signature of known viruses because the signature is for identifying infected programs from another signature in order to provide a solution or antivirus program.

As per claim 49:

Freund teaches a computerized method comprising determining an active networked application [col.10, lines 31-44 and col.30, lines 13-15] and filtering a set of intrusion rules to create a subset of intrusion rules corresponding to the active networked application [col.4, lines 65-67 and col.5, lines 39-43], where the subset of the intrusion rules corresponding to the active networked application are capable of being used for evaluating intrusions that target the corresponding active networked application [col.5, lines 46-59 and col.8, lines 45-52].

Kaler, et al. teaches the an invention that includes a number of different aspects for analyzing the performance of a data processing system wherein provides the filtering process and filter reduction feature. Kaler disclose the filter defines what information it (VSA) will collect and analyze (col.23, lines 14-15) and the filter reduction is the process of modifying or creating a new version of a Boolean expression (col.23, lines 45-65) whereby extracts only the

information of interest so that it reduces the performance impact of monitoring or processing resources (col.4, lines 57-61).

Freund and Kaler combinations did not include signature of known attacks in the set of intrusion rules. However, it is known in the art that signature of known attacks are also known as virus signatures. A signature is known as a unique computer code contained in a virus and that the signature for a known attacks or viruses is to identify infected programs or files and by knowing the signature of the attack will help find the antivirus program.

Therefore it would have been obvious for a person of ordinary skills in the art to combine the teachings of Freund and Kaler with Official Notice that signature of known viruses because the signature is for identifying infected programs from another signature in order to provide a solution or antivirus program.

(10) Response to Argument

Issue #1:

The rejection under 35 U.S.C.112, 1st paragraph for claim 51 is withdrawn. Freund reads on the claimed the information associated with an active networked application making a new connection never previously made because Freund discloses the applications panel displays a new node for indicating the new executing process and each driver is responsible for monitoring and filtering access for its particular type, including ensuring that any user activity which employs that access type conforms to any rules or conditions specified for the Internet monitor (col.23, lines 20-22 and 52-55).

Issue #2:

Group #1: claims 1, 7-12, 14-15, 21-26, 28-29, 35-40, 42-43, 47, and 50

With respect to the first element of the *prima facie* case of obviousness:

The examiner traverses appellant's argument where Kaler's invention does not teach away from any sort of security system by stating "without degrading its data security characteristics" (abstract). The below (paragraphs) will explain further the Freund's and Kaler's invention that includes monitoring and the process of filtering for active networked applications.

Freund teaches a system and method for client based monitoring and filtering (col.3, lines 50-67). Freund discloses that applications (software) can be a Web browser (i.e. Netscape Navigator or Microsoft Internet Explorer) which communicates with the Internet (col.8, lines 2-10 and col.15, lines 14-21). An active application is where active use occurs when a user directly interacts with an Internet application while that application accesses the Internet (col.10, lines 17-43). Freund discloses client-based filter application performs all of the monitoring, logging, filter work, and also keeps a list of currently active processes and determines which process is actively used (col.4, lines 31-37). Freund discloses the system can monitor TCP/IP activities on a per process or per application basis and it access rights (col.4, lines 52-55). Freund discloses the set of intrusion rules are access rules for the entire LAN for one or more workgroups, or the specific user (col.3, lines 61-63). These access rules include criteria in the form of subset of intrusion rules (col.4, lines 9-27 and col.5, lines 39-43) corresponding to the active networked application.

Kaler identifies a known problem with performance analysis for data processing systems is that very often such analysis provides opportunities for breaching the data security of such systems (col.2, lines 64-67). Thus, Kaler indicates there is a substantial need to provide automated tools for efficiently analyzing the performance, function and behavior of their applications without significantly affecting the performance or data security characteristics of the applications (col.3, lines 39-45). Kaler includes filter(s) for event monitoring that is a way in which the system user can specify what is to be monitored in the system under examination

(col.22, lines 2-4). Kaler discloses filtering a set of intrusion rules in the form of triggers that are set to monitor for a selected condition or error to occur (col.21, lines 47-52). Kaler provides a secure environment for data collection through the use of discretionary access controls such that discretionary access controls may be based on authentication identities and encryption techniques (col.22, line 53-col.23, line 7). Hence, the subset of rules is from a process of filter reduction that extract portions of a filter relevant to specify a specific portion of the monitoring infrastructure (col.4, lines 56-61 and col.23, lines 34-45).

By reading further into the Kaler reference, appellant's points to "without modifying or degrading its data security characteristics" to show this teaches away from a security system. However, this recitation is actually an advantage instead of a disadvantage to a security system because Kaler suggests that there is a substantial need to provide automated tools for efficiently analyzing the performance, function and behavior of their applications without significantly affecting the performance or data security characteristics of the applications (col.3, lines 39-45). This merely shows that Kaler's method will not affect the security or lower its standard for its data security characteristics and still maintain the flow and performance of the application. Thus, without modifying or degrading its performance or data security characteristics teaches an added benefit to the security prevention. Therefore, Kaler's invention does have suggestions of security for the system (col.21, lines 46-52 and col.22, lines 45-55 and col.23, lines 1-8). Thus, Kaler does not teach away from any sort of security system. Kaler is a proper secondary prior art in combination with Freund because the Freund and Kaler combination meets the first (element) basic criteria of "there must be some suggestion or motivation, either in the references themselves or in the knowledge generally available to one of ordinary skills in the art to modify the references or to combine reference teachings".

Page 12, 1st & 2nd paragraph of brief:

With respect to the third element of the *prima facie* case of obviousness:

In regards to "rules corresponding to the active networked application". Freund discloses applications (software) can be a Web browser (i.e. Netscape Navigator or Microsoft Internet Explorer) which communicates through a communication layer or driver with the Internet (col.8, lines 2-10 and col.15, lines 14-21). Freund discloses an active use occurs when a user directly interacts with an Internet application while that application accesses the Internet (col.10, lines 17-43). Rules can be interpreted as given permissions, restrictions, or certain criteria for certain users, workstations, or applications such that rules are for regulating access or activity. Freund discloses access rules include criteria or subset of rules (col.5, lines 39-43) where the subset rules includes a list of applications or application versions that a user can/cannot use, list of URLs that the application can/cannot use, or a list of protocols or protocol component an application can/cannot use (col.4, lines 9-27). These rules corresponds to the active networked application. Therefore, Freund teaches the claimed rules corresponding to the active networked application.

Page 12, 3rd paragraph of brief:

In regards to "filtering a set of intrusion rules to create a subset of intrusion rules corresponding to the active networked application". Examiner traverses that Freund does not mention any sort of filtering. The filtering application involves monitoring, logging, and filtering work (col.3, lines 51-52 and col.4, lines 29-32). Freund discloses filtering as the ability to monitor and regulate Internet access on a per application basis by determining which applications can/cannot access the Internet (col.4, lines 19-28 and col.10, lines 55-65). Filtering can be interpreted as sorting or looking for certain attributes or criteria. Rules regulates access

such that rules can broadly be any permissions and restrictions or having specific attributes or criteria to indicate allowed access or unsafe.

Freund discloses intrusion rules in the form of access rules referring to one or more workgroups or users (col.3, lines 62-63 and col.4, lines 5-8). The access rules are specific to workstations/users that is allowed to have access to the Internet (col.5, lines 10-12 and 23-41) or that is used to block all clients that have not been verified (col.4, lines 1-3). Freund further discloses filtering the access rules sorts out the certain user/workstation allowed access or restricted access to the Internet to create filtered subset of rules (col.5, lines 39-43 and col.9, lines 4-13). These subset of intrusion rules corresponds to the active networked applications because the rules pertain to applications that can/cannot access the Internet, protocols that the application can/cannot use (col.4, lines 13-18) or applications with known security problems (col.6, lines 1-3). Thus, this obviously suggest filtering a set of intrusion rules creating subset of intrusion rules. The networked application is active when there are users/workstations interacting to the Internet using web browser (col.6, lines 8-15 and col.10, lines 18-20) and when the application is being monitored because the application is attempting to get access to the Internet (col.10, lines 55-58). Thus, this obviously suggests active networked application and reads on the claimed filtering intrusion rules to create a subset of intrusion rules corresponding to the active networked application.

Another example of filtering a set of intrusion rules to create a subset of rules corresponding to the active networked application. Freund discloses comparing application properties (i.e. version, executable name) with the database of application allowed to access the Internet and checks what kind of activity (i.e. mail, browsing) the application is allowed to do (col.5, lines 55-60). The database obviously contain subset of intrusion rules since it is the application properties that is being compared to determine if the application is allowed access to

the Internet or if violating any rules (col.5, lines 46-52). The a set of intrusion rules is in the form of application properties such having the version type/number, executable name, and the like to allow access to the Internet. For instance, filtering the set of intrusion rules involves looking for the permitted application version type A to see if the specified attributes matches to the database of application allowed access to the Internet. The filtering of application properties indicates the application version type A is allowed to access the internet which now creates the subset of rules for this version type A. The subset of rules indicates the kind of activity such as the application is allowed to browse (col.5, lines 55-60). Another example is comparing the application properties with the database of application with known security problems (col.6, lines 1-3) where the certain version type or executable name has attributes of the database with application with known security problems is detected, then the subset of rules is to stop the application from accessing the Internet and/or warns the user (col.6, lines 4-7). The networked application is active because Freund discloses the application attempts to access Internet (col.5, lines 55 and 67).

Page 12, 4th & 5th paragraph of brief:

The Advisory Action (3/15/2006) briefly discusses the Kaler reference. Thus, the Final Office Action (11/15/2005) better explains the Freund and Kaler combination. Freund discloses filtering creating the subset of intrusion rules corresponding to the active networked application but fails to further explain details of the subset of intrusion rules are used for reducing a required amount of processing resources. Thus, Kaler is brought forth to teach this limitation. As discussed previously, Freund is the primary reference brought forth disclosing the claimed filtering (col.4, lines 29-32 and col.10, lines 55-65) a set of intrusion rules (col.3, lines 61-63 and col.4, lines 1-3) to create a subset of intrusion rules (col.4, lines 5-27 and col.6, lines 1-3) corresponding to the active networked application (col.10, lines 17-43).

In the Advisory Action (3/15/2006), states that Freund does have the claimed "filtering rules". However, the examiner meant subset rules corresponding to the active networked application because the claimed invention does not recite "filtering rules corresponding to the active networked application". The claimed invention recites filtering a set of intrusion rules to create the subset of intrusion rules corresponding to the active networked application. Thus, the set of intrusion rules have not limited to applications, users, or workstations whereas the subset of intrusion rules limits to only applications. As such, Freund's intrusion rules may apply to the user/workstation (col.3, lines 61-65 and col.5, lines 39-60). The user/workstation have access to certain applications where those applications have certain access (subset of intrusion rules) to access the Internet (col.4, lines 5-27).

Page 13 of brief:

The examiner have responded to the argument pertaining to "filtering a set of intrusion rules to create a subset of intrusion rules corresponding to the active networked application". This reflects the same argument on Page 12, 3rd paragraph of brief.

Freund discloses the subset of intrusion rules (i.e. mail, browsing, or stop from accessing the internet and warns user) are stored in the databases are compared to when application attempts to access Internet (col.5, lines 55 – col.6, line 15). Thus, the subset of intrusion rules can be used for evaluating intrusions that target the corresponding active networked application against the database of applications with known security problems (col.6, lines 1-3). The application is active because it is attempting to access the Internet (col.6, lines 4-7). Therefore, this reads on subset of the intrusion rules corresponding to the active networked application are capable of being used for evaluating intrusion that target the corresponding active networked application (col.5, lines 45-51 and col.6, lines 5-15).

Page 14 of brief:

Appellant referencing col.5, lines 46-59 and col.8, lines 45-52 does not only relate to accessing the internet including rules associated with applications that are allowed to access the Internet. Col.5, lines 39-60 explains specifying rules which govern Internet access, transmitting a filtered subset of the rules to the particular client, and the process of determining whether the request to access the Internet would violate any rules. This shows the filtering a set of intrusion rules to create the subset of intrusion rules corresponding to the active networked application.

The examiner traverses that Freund fails to disclose a technique where the subset of the intrusion rules corresponding to the active networked application are capable of being used for evaluating intrusions that target the corresponding active networked application. The examiner have discussed above in section Page 13, 2nd paragraph.

Page 15 of brief:

Col.10, lines 18-50 explains the networked application is active by the interaction of a user. Freund also discloses the application is being monitored is active because the application is attempting to access the Internet. Freund discloses the evaluating intrusions of an active networked application with the ability to monitor and regulate Internet access by specifying which applications can or cannot access the Internet (col.10, lines 55-58). Freund further explains the monitoring access to the Internet by individual applications allowing the system to not only track Internet traffic but determine data exchanged on a per application basis including the ability to determine the name of individual files downloaded. The approach creates an audit trail of download files thus allowing one to trace the source of files found to contain offensive contents or pose security risks (col.11, lines 1-18). Another form of evaluating intrusions is where Freund discloses the subset of intrusion rules (i.e. mail, browsing, or stop from accessing

the internet and warns user) are stored in the databases are compared to when application attempts to access Internet (col.5, lines 55 – col.6, line 15). Thus, the subset of intrusion rules can be used for evaluating intrusions that target the corresponding active networked application against the database of applications with known security problems (col.6, lines 1-3). The application is active because it is attempting to access the Internet (col.6, lines 4-7). Therefore, this reads on subset of the intrusion rules corresponding to the active networked application are capable of being used for evaluating intrusion that target the corresponding active networked application (col.5, lines 45-51 and col.6, lines 5-15).

The Freund and Kaler combination:

Freund discloses intrusion rules is in the form of access rules refers to one or more workgroups or users (col.3, lines 62-63 and col.4, lines 5-8). The access rules are specific to workstations/users that are allowed to have access to the Internet (col.5, lines 10-12 and 23-41) or to block all clients that have not been verified (col.4, lines 1-3). Freund further discloses filtering the access rules sorts out the certain user/workstation allowed access or restricted access to the Internet to create filtered subset of rules (col.5, lines 39-43 and col.9, lines 4-13). These subset of intrusion rules corresponds to the active networked applications because the rules pertains to applications that can/cannot access the Internet, protocols that the application can/cannot use (col.4, lines 13-18) or applications with known security problems (col.6, lines 1-3). Thus, this obviously suggests filtering a set of intrusion rules creating subset of intrusion rules. The networked application is active when there are users/workstations interacting to the Internet using web browser (col.6, lines 8-15 and col.10, lines 18-20) and when the application is being monitored because the application is attempting to get access to the Internet (col.10, lines 55-58). Thus, this obviously suggest active networked application and reads on the claimed filtering intrusion rules to create a subset of intrusion rules corresponding to the active

networked application. Freund discloses the subset of intrusion rules corresponding to the active networked application but fails to further explain details of the subset of intrusion rules are used for reducing a required amount of processing resources.

It is obvious the subset of intrusion rules is reduced or narrowed down to certain criteria for evaluation corresponding to the active network application. Hence, Kaler teaches filter reduction is used to narrow the scope of the filter to extract only the information of interest and hence reduce the performance impact of monitoring results the subset of intrusion rules (col.4, lines 56-61 and col.23, lines 34-45). Therefore it would have been obvious for a person of ordinary skills in the art at the time of the invention to combine the teaching of filtering a set of intrusion rules to create a subset of intrusion rules corresponding to the active networked application of Freund with the teaching of filter reduction as taught by Kaler because the subset of rules is by narrowing the scope of the filter to extract only the information of interest and hence reduce the performance impact of monitoring.

Group #2: claims 2, 16, 30, and 44

Freund discloses detecting when the active networked application becomes inactive is when there are violated rules for the attempt to access the Internet because the communication is terminated or stops the application from accessing the Internet (col.4, lines 59-61 and col.5, lines 60-63). Thus, its is obvious that if the application is terminated from communicating or accessing the Internet is when the application becomes inactive. Freund also discusses re-filtering by redirecting the access after the violated rules occurred (col.4, lines 27-28).

Group #3: claims 3-4, 17-18, and 31-32

Freund discloses tracking Internet activity and the ability to monitor and regulate access for applications that includes specifying which applications can or cannot access the Internet (col.10, lines 45-58). So when an application attempting to access the Internet and violated

rules, the application is denied access and stops the application from accessing the Internet (col.5, lines 61-64). Thus, it's obvious that Freund monitors both when access is allowed and connection termination once the application is stopped from accessing the Internet.

Group #4: claims 3-4, 17-18, and 31-32

These dependent claims are rejected with new grounds of rejection which now involves the prior art of Hanko, et al. The Freund and Kaler combination did not include detecting when no networked application is active, and suspending the evaluating of network traffic until a networked application is active.

Hanko, et al. teaches a method and apparatus for improving utilization of one or more resources in a share client computer environment (col.3, lines 30-32). Hanko points out that on a consolidated client system, a small load may be multiplied by tens, hundreds, or even millions of users of the shared system, can consume all of the resources of the shared system, even when no real work is being done (col.5, lines 1-8). Hanko discloses using traditional computer programs on a shared client by monitoring the status of an application, determining when an application no longer needs resources and causing the application to stop consuming resources (col.3, lines 34-37). The invention has a mechanism to stop a program from consuming resources when it detects a user has stopped interaction with an application and to restart it when the user begins interaction with it (col.5, lines 21-28). When there is no interaction regarding the application, it becomes inactive (col.5, lines 10-13). This inactive application no longer consumes resources and is not being evaluated or suspended for the time being until the application returns to its original (active) state again (col.12, lines 33-45 and 55-62). Therefore, it would have been obvious for a person of ordinary skills in the art at the time of the invention was made to combine the teaching of monitoring and filtering with intrusion rules of the Freund and Kaler with the teaching of causing the application to stop consuming resources when

detecting an application is inactive and to restart when the application active (col.3, lines 45-52) because this improves resource utilization (col.4, lines 16-17).

Group #5: claim 48

The claim recites the intrusion rules include information selected from the group of consisting of a target active networked application, a specific hostile payload, a network port or protocol.

Freund discloses monitoring access to the Internet by individual applications allows the system to not only track Internet traffic but also can determine data exchanged on a per application basis including the ability to determine the name of individual files downloaded as well as target directories to where such files are copied. This approach creates an audit trail of downloaded files thus allowing one to trace the source files found to contain offensive contents or pose security risks (col.11, lines 9-18). Freund includes access rules in the monitoring and filtering invention to determine what the user/workstation and the application can or cannot access. The cannot access is considered to intrusion of Freund's access rules. The can or cannot access rules includes a list of protocols or protocol components and list of applications or application versions (col.4, lines 13-18). Freund further include displaying a selection of actions to undertake in the event that a rule is violated (col.26, lines 45-65). The examples are denying Internet access or issue a warning (col.4, lines 26-28). Thus, Freund reads on the limitation of claim 48.

Group #6: claim 51

The rejected under 35 U.S.C.112, 1st paragraph for claim 51 is withdrawn. Freund discloses the applications panel displays a new node for indicating the new executing process and each driver is responsible for monitoring and filtering access for its particular type, including ensuring that any user activity which employs that access type conforms to any rules or

conditions specified for the Internet monitor (col.23, lines 20-22 and 52-55). This recitation reads on the claimed the information associated with an active networked application making a new connection never previously made.

Issue #3:

Claims 13, 27, 41, and 49 are rejected under 35 U.S.C. 103(a) as being unpatentable over Freund and Kaler, and further in view of Official Notice.

The examiner have previously established that both Freund and Kaler teaches an inventions that include monitoring and the process of filtering for active networked applications that involves security. However, Freund and Kaler combinations did not include signature of known attacks in the set of intrusion rules. It is known in the art that signature of known attacks are also known as virus signatures. A signature is known as a unique computer code contained in a virus and that the signature for a known attacks or viruses is to identify infected programs or files and by knowing the signature of the attack will help find the antivirus program. Therefore it would have been obvious for a person of ordinary skills in the art to combine the teachings of Freund and Kaler with Official Notice that signature of known viruses because the signature is for identifying infected programs from another signature in order to provide a solution or antivirus program.

As such, the examiner have provide the third element of the prima facie case of obviousness because the prior art references in combination teach or suggest all of the claimed limitations.

(11) Related Proceeding(s) Appendix

No decision rendered by a court or the Board is identified by the examiner in the Related Appeals and Interferences section of this examiner's answer.

For the above reasons, it is believed that the rejections should be sustained.

This examiner's answer contains a new ground of rejection set forth in section **(9)** above. Accordingly, appellant must within **TWO MONTHS** from the date of this answer exercise one of the following two options to avoid *sua sponte* **dismissal of the appeal** as to the claims subject to the new ground of rejection:

(1) **Reopen prosecution.** Request that prosecution be reopened before the primary examiner by filing a reply under 37 CFR 1.111 with or without amendment, affidavit or other evidence. Any amendment, affidavit or other evidence must be relevant to the new grounds of rejection. A request that complies with 37 CFR 41.39(b)(1) will be entered and considered. Any request that prosecution be reopened will be treated as a request to withdraw the appeal.

(2) **Maintain appeal.** Request that the appeal be maintained by filing a reply brief as set forth in 37 CFR 41.41. Such a reply brief must address each new ground of rejection as set forth in 37 CFR 41.37(c)(1)(vii) and should be in compliance with the other requirements of 37 CFR 41.37(c). If a reply brief filed pursuant to 37 CFR 41.39(b)(2) is accompanied by any amendment, affidavit or other evidence, it shall be treated as a request that prosecution be reopened before the primary examiner under 37 CFR 41.39(b)(1).

Extensions of time under 37 CFR 1.136(a) are not applicable to the TWO MONTH time period set forth above. See 37 CFR 1.136(b) for extensions of time to reply for patent applications and 37 CFR 1.550(c) for extensions of time to reply for ex parte reexamination proceedings.

Respectfully submitted,

LH

Leynna Ha

A Technology Center Director or designee must personally approve the new ground(s) of rejection set forth in section (9) above by signing below:

Conferees:

Kim Vu KV

Kambiz Zand

Zilka-Kotab, P.C.

P.O. Box 721120

San Jose, California 95172-1120

PETER WONG, DIRECTOR
TECHNOLOGY CENTER 2100